

**IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRCIT OF PENNSYLVANIA**

**IN RE PHILADELPHIA INQUIRER
DATA SECURITY LITIGATION**

Case No. 2:24-CV-2106-KSM

**CONSOLIDATED CLASS
ACTION COMPLAINT**

JURY TRIAL DEMANDED

Plaintiffs Christopher Devine, Steven Hassell, and Ivery Sheree Mosley (“Plaintiffs”), individually and on behalf of all others similarly situated (“Class Members”), bring this class action against Defendant The Philadelphia Inquirer, LLC (“The Inquirer” or “Defendant”). The allegations set forth in this Complaint are based on Plaintiffs’ personal knowledge as to his own actions and experiences, and upon information and belief and further investigation of counsel.

INTRODUCTION

1. This action arises from Defendant’s recent data breach (“Data Breach”) resulting from its failure to implement reasonable and industry standard data security practices.
2. Defendant is the purveyor of a daily newspaper which circulates throughout Pennsylvania, Delaware, New Jersey, and Maryland reaching more than 350,000 people every day.¹
3. Plaintiffs brings this Complaint against Defendant for its failure to properly secure and safeguard the sensitive information that it collected and maintained as part of its regular business practices, including, but not limited to: names, Social Security numbers, Driver’s license or state ID numbers, financial account information, credit card numbers, debit card numbers,

¹ <https://www.infoplease.com/culture-entertainment/journalism-literature/top-100-newspapers-united-states>

medical and health information, and account usernames, passwords, and other access codes (“Private Information”).

4. Upon information and belief, former and current subscribers to, and employees at, the Inquirer are required to entrust Defendant with sensitive, non-public Private Information, without which Defendant could not perform its regular business activities. Defendant retains this information for at least many years and even after the relationship has ended.

5. By obtaining, collecting, using, and deriving a benefit from the Private Information of Plaintiffs and Class Members, Defendant assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion.

6. Plaintiffs received a Notice of Data Breach letter (the “Notice Letter”) from Defendant on or about April 29, 2024. According to this Notice Letter, Defendant learned of a cybersecurity incident on May 11, 2023, and pursued an investigation into the threat.² After the incident was initially detected, it took several days for Defendant to correct the problem and secure its systems.

7. Defendant's investigation concluded that the unauthorized actor was able to access and exfiltrate certain of Plaintiffs' and Class Members' Private Information, including Social Security numbers, financial information, account passwords, and healthcare information.³

8. Defendant failed to adequately protect Plaintiffs' and Class Members' Private Information—and failed to even encrypt or redact this highly sensitive information. This unencrypted, unredacted Private Information was compromised due to Defendant's negligent

² The “Notice Letter”

³ “Hackers may have accessed Inquirer subscribed and employee personal data in 2023 cyberattack,” *The Philadelphia Inquirer*, available at <https://www.inquirer.com/news/philly-inquirer-cyberattack-personal-data-20240426.html>

and/or careless acts and omissions and their utter failure to protect its employees' and subscribers' sensitive data. Hackers targeted and obtained Plaintiffs' and Class Members' Private Information because of its value in exploiting and stealing the identities of Plaintiffs and Class Members. The present and continuing risk to victims of the Data Breach will remain for their respective lifetimes.

9. In breaching its duties to properly safeguard its employees' and subscribers' Private Information and give the victims timely, adequate notice of the Data Breach's occurrence, Defendant's conduct amounts to negligence and/or recklessness and violates federal and state statutes.

10. Indeed, although Defendant discovered the Data Breach in May 2023, it did not disclose it until nearly a year later, publishing an article on April 26, 2024, and sending notice to Plaintiffs and Class Members on or about April 29, 2024.

11. Plaintiffs brings this action on behalf of all persons whose Private Information was compromised as a result of Defendant's failure to: (i) adequately protect the Private Information of Plaintiffs and Class Members; (ii) warn Plaintiffs and Class Members of Defendant's inadequate information security practices; and (iii) effectively secure hardware containing protected Private Information using reasonable and effective security procedures free of vulnerabilities and incidents. Defendant's conduct amounts at least to negligence and violates federal and state statutes.

12. Defendant disregarded the rights of Plaintiffs and Class Members by intentionally, willfully, recklessly, or negligently failing to implement and maintain adequate and reasonable measures to ensure that the Private Information of Plaintiffs and Class Members was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required, and appropriate protocols, policies, and procedures regarding the encryption

of data, even for internal use. As a result, the Private Information of Plaintiffs and Class Members was compromised through disclosure to an unknown and unauthorized third party. Plaintiffs and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

13. Plaintiffs and Class Members have suffered injuries as a result of Defendant's conduct. These injuries include: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) experiencing an increase in spam calls, texts, and/or emails; (viii) statutory damages; (ix) nominal damages; and (x) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

14. Plaintiffs seeks to remedy these harms and prevent any future data compromise on behalf of himself and all similarly situated persons whose personal data was compromised and stolen as a result of the Data Breach and who remain at risk due to Defendant's inadequate data security practices.

PARTIES

15. Plaintiff Christopher Devine is and has been, at all relevant times, a resident and citizen of Corryton, Tennessee. Plaintiff Devine received the Notice Letter, via U.S. mail, directly from Defendant, dated April 29, 2024.

16. Plaintiff Steven Hassell is and has been, at all relevant times, a resident and citizen of Philadelphia, Pennsylvania. Plaintiff Hassell received the Notice Letter, via U.S. mail, directly from Defendant, dated April 29, 2024.

17. Plaintiff Ivery Sheree Mosley is and has been, at all relevant times, a resident and citizen of Brookhaven, Pennsylvania. Plaintiff Mosley received the Notice Letter, via U.S. mail, directly from Defendant, dated April 29, 2024.

18. Defendant The Philadelphia Inquirer is a Delaware limited liability company with its principal place of business located at 100 S. Independence Mall West, Suite 600, Philadelphia, PA 19106. The Philadelphia Inquirer LLC is owned by the Lenfest Institute, a non-profit operating from its primary headquarters at 100 S. Independence Mall West, Suite 600, Philadelphia, PA 19106.

JURISDICTION AND VENUE

19. This Court has subject matter jurisdiction as a court of general jurisdiction.

20. This Court has personal jurisdiction over Defendant because it operates and maintains its principal place of business within Philadelphia County.

21. Venue is proper in this District because Defendant's principal place of business is located in this district; Defendant maintains Class Members' Private Information in this District; and Defendant caused harm to Class Members residing in this District.

STATEMENT OF FACTS

Defendant's Business

22. Defendant is a company which provides local, national, and international news services to individuals living in the greater Philadelphia area.⁴

⁴ <https://about.inquirer.com/>

23. In order to obtain services from Defendant, Defendant requires its subscribers to provide sensitive and confidential Private Information, including names, addresses, and payment or financial information. Similarly, to obtain employment by Defendant, applicants must disclose their sensitive and confidential Private Information as well, including their names, addresses, Social Security numbers, and driver's licenses or state ID numbers.

24. The information held by Defendant in its computer systems included the unencrypted Private Information of Plaintiffs and Class Members.

25. Upon information and belief, Defendant made promises and representations to its employees and subscribers that the Private Information collected from them as a condition of obtaining employment or services from Defendant would be kept safe, confidential, that the privacy of that information would be maintained, and that Defendant would delete any sensitive information after it was no longer required to maintain it.

26. Plaintiffs and Class Members provided their Private Information, directly or indirectly, to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

27. Plaintiffs and the Class Members have taken reasonable steps to maintain the confidentiality of their Private Information. Plaintiffs and Class Members relied on the sophistication of Defendant to keep their Private Information confidential and securely maintained, to use this information for necessary purposes only, and to make only authorized disclosures of this information. Plaintiffs and Class Members value the confidentiality of their Private Information and demand security to safeguard their Private Information.

28. Defendant had a duty to adopt reasonable measures to protect the Private Information of Plaintiffs and Class Members from involuntary disclosure to third parties. Defendant has a legal duty to keep its employees' and subscribers' Private Information safe and confidential.

29. Defendant had obligations created by the FTC Act, HIPAA, Pennsylvania's Unfair Trade Practices and Consumer Protection Law ("UDPCPL"), Pennsylvania's Personal Information Breach Notification Act, contract, and industry standards, to keep its employees' and subscribers' Private Information confidential and to protect it from unauthorized access and disclosure.

30. Defendant derived a substantial economic benefit from collecting Plaintiffs' and Class Members' Private Information. Without the required submission of Private Information, Defendant could not perform the services it provides.

31. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' Private Information, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiffs' and Class Members' Private Information from disclosure.

Defendant's Data Breach

32. On April 26, 2024, Defendant published an article (the "Article") in its paper and on its digital platform disclosing the Data Breach, reading, in pertinent part:

About 25,500 Philadelphia Inquirer subscribers, employees, former employees, and employees' family members on company benefit plans may have had their personal information exposed in a May cyberattack, Inquirer publisher and chief executive officer Lisa Hughes said Friday.

The company announced in an internal email to employees that outside cybersecurity experts had found no evidence that the data had been misused to commit identity theft or fraud. In an e-mailed response to follow-up questions, Hughes said that Social Security numbers, driver's license numbers, financial account information, and medical information may have been accessed.

...

The update comes at the conclusion of what The Inquirer called a “complex, methodical, and lengthy process” to investigate the incident.

The investigation was unable to identify the specific individual or individuals who were behind the attack or their motivations, Hughes said. She declined to share what files may have been impacted, citing confidentiality reasons.

Cyberattacks, which have more than doubled in recent years, pose a major threat to businesses, governments, and consumers around the world.

Locally over the past year, the City of Philadelphia, Pennsylvania Courts, the Bucks County Department of Emergency Management, Comcast, and the Borgata in Atlantic City have responded to attacks, some of which severely disrupted operations for days and potentially exposed people’s confidential health and financial information.

The Inquirer’s cyberattack

The incident at The Inquirer was detected on May 11, 2023, when Cynet, a vendor that manages security, alerted the company of suspicious network activity. By May 13, 2023, some of the Inquirer’s publishing systems were impacted, and workarounds had to be created to post stories online.

In the days after the incident, Hughes said The Inquirer had “discovered anomalous activity on select computer systems and immediately took those systems off-line.” The company also notified the FBI.

...

A ransomware group called Cuba, which has hacked other businesses and governments around the globe, later claimed responsibility for the attack, and posted online what it said were stolen Inquirer files containing Inquirer data. A day later, however, Cuba removed the claim from its site on the dark web. Hughes at the time said the company had not seen evidence that any Inquirer information was actually shared. When asked at the time, she did not say whether The Inquirer had paid a ransom in exchange for the claim’s removal.

In recent years, ransomware attacks have targeted news organizations, including the Los Angeles Times, which was majorly disrupted during a 2018 attack. In these incidents, malicious software locks users out of their system and demands payment to reopen it.

In the months since the Inquirer's incident, the company has increased digital security, including by requiring multifactor authentication on its systems.

"The Inquirer takes this event and the security of information in its care very seriously," Hughes said. "The Inquirer regularly evaluates the evolving risk landscape and implements controls to mitigate those risks."⁵

33. The Article does not disclose the root cause of the Data Breach, and notably withholds information about whether any ransom was paid to protect the information of Defendants' employees and subscribers.

34. The Article does make clear that news organizations have frequently been targeted in recent years by ransomware attacks from cyber criminals, and that Defendant "takes this even and the security of information in its care very seriously."

35. Still, Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive information it was maintaining for Plaintiffs and Class Members, causing the exposure of Private Information, such as encrypting the information or deleting it when it is no longer needed.

36. Defendant also failed to notify the victims of this Data Breach of its occurrence until nearly a full year after it transpired, leaving Defendant's employees and subscribers unknowingly vulnerable to fraud and identity theft for nearly twelve whole months.

37. The attacker accessed and acquired files in Defendant's computer systems containing unencrypted Private Information of Plaintiffs and Class Members, including their names, addresses, payment information, account information, Social Security numbers, healthcare information, and potentially other sensitive information. Plaintiffs' and Class Members' Private Information was accessed and stolen in the Data Breach.

⁵ <https://www.inquirer.com/news/philly-inquirer-cyberattack-personal-data-20240426.html>

38. Plaintiffs further believes that his Private Information and that of Class Members was or will be sold on the dark web, as the ransomware group Cuba claimed credit for the attack and already posted the files to the Dark Web, as acknowledged by Defendant.⁶

Data Breaches Are Preventable

39. As explained by the Federal Bureau of Investigation, “[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection.”⁷

40. To prevent and detect cyber-attacks and/or ransomware attacks Defendant could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.

⁶ <https://www.inquirer.com/news/philly-inquirer-ransomware-cuba-fbi-20230523.html>

⁷ See How to Protect Your Networks from RANSOMWARE, at 3, available at <https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view>

- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.
- Consider disabling Remote Desktop protocol (RDP) if it is not being used.
- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment.
- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.⁸

41. To prevent and detect cyber-attacks or ransomware attacks Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

Secure internet-facing assets

- Apply latest security updates
- Use threat and vulnerability management
- Perform regular audit; remove privileged credentials;

Thoroughly investigate and remediate alerts

- Prioritize and treat commodity malware infections as potential full compromise;

Include IT Pros in security discussions

⁸ *Id.* at 3-4.

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

Build credential hygiene

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords;

Apply principle of least-privilege

- Monitor for adversarial activities
- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events;

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office[Visual Basic for Applications].⁹

42. Given that Defendant was storing the sensitive Private Information of its current and former employees and subscribers, Defendant could and should have implemented all of the above measures to prevent and detect cyberattacks.

43. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breach and the exposure of the Private Information of over two million individuals, including that of Plaintiffs and Class Members.

⁹ See Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), available at: <https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/>

Defendant Acquires, Collects, & Stores Plaintiffs' and Class Members' Private Information

44. As a condition to obtain services and/or employment from Defendant, The Inquirer requires its employees' and subscribers to give their sensitive and confidential Private Information to Defendant.

45. Defendant retains and store this information and derive a substantial economic benefit from the Private Information that they collect. But for the collection of Plaintiffs' and Class Members' Private Information, Defendant would be unable to perform its services.

46. By obtaining, collecting, and storing the Private Information of Plaintiffs and Class Members, Defendant assumed legal and equitable duties and knew or should have known that they were responsible for protecting the Private Information from disclosure.

47. Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their Private Information and relied on Defendant to keep their Private Information confidential and maintained securely, to use this information for business purposes only, and to make only authorized disclosures of this information.

48. Defendant could have prevented this Data Breach by properly securing and encrypting the files and file servers containing the Private Information of Plaintiffs and Class Members.

49. Upon information and belief, Defendant made promises to its employees and subscribers that it would maintain and protect their Private Information, demonstrating an understanding of the importance of securing Private Information.

50. Indeed, Defendant stated in the aftermath of the attack, roughly a year after its occurrence, “The Inquirer takes this event and the security of information in its care very seriously.”¹⁰

51. Defendant's negligence in safeguarding the Private Information of Plaintiffs and Class Members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

Defendant Knew, Or Should Have Known, Of The Risk Because Software Companies In Possession Of Private Information Are Particularly Susceptible To Cyber Attacks

52. Data thieves regularly target companies like Defendant's due to the highly sensitive information that they custody. Defendant knew and understood that unprotected Private Information is valuable and highly sought after by criminal parties who seek to illegally monetize that Private Information through unauthorized access.

53. Defendant's data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches targeting software companies that collect and store Private Information and other sensitive information, like Defendant, preceding the date of the breach.

54. In the third quarter of the 2023 fiscal year alone, 7333 organizations experienced data breaches, resulting in 66,658,764 individuals' personal information being compromised.¹¹

55. Defendant itself acknowledged that ransomware attacks against news and media organizations are common, impacting organizations such as the Los Angeles Times (2018), the Guardian (2022), Norway's Amedia (2021), and The Sun (2019).

¹⁰ <https://www.inquirer.com/news/philly-inquirer-cyberattack-personal-data-20240426.html>

¹¹ See <https://www.idtheftcenter.org/publication/q3-data-breach-2023-analysis/>

56. In a survey conducted in 2023 by Sophos, a leader in cybersecurity, 100 out of 138 leaders at media and entertainment businesses disclosed that their companies had been targeted by ransom attacks in the past year alone.¹²

57. Indeed, cyber-attacks, such as the one experienced by Defendant, have become so notorious that the Federal Bureau of Investigation (“FBI”) and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. As one report explained, smaller entities that store Private Information are “attractive to ransomware criminals...because they often have lesser IT defenses and a high incentive to regain access to their data quickly.”¹³

58. Additionally, as companies became more dependent on computer systems to run their business,¹⁴ e.g., working remotely as a result of the Covid-19 pandemic, and the Internet of Things (“IoT”), the danger posed by cybercriminals is magnified, thereby highlighting the need for adequate administrative, physical, and technical safeguards.¹⁵

59. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the Private Information of Plaintiffs and Class Members from being compromised.

60. As a custodian of Private Information, Defendant knew, or should have known, the importance of safeguarding the Private Information entrusted to it by Plaintiffs and Class members,

¹² <https://pressgazette.co.uk/publishers/digital-journalism/news-publishers-cyberattacks-hackers/>

¹³https://www.law360.com/consumerprotection/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware?nl_pk=3ed44a08-fcc2-4b6c-89f0-aa0155a8bb51&utm_source=newsletter&utm_medium=email&utm_campaign=consumerprotection

¹⁴<https://www.federalreserve.gov/econres/notes/feds-notes/implications-of-cyber-risk-for-financial-stability-20220512.html>

¹⁵ <https://www.picussecurity.com/key-threats-and-cyber-risks-facing-financial-services-and-banking-firms-in-2022>

and of the foreseeable consequences if its data security systems were breached, including the significant costs imposed on Plaintiffs and Class Members as a result of a breach.

61. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the Private Information of Plaintiffs and Class Members and of the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiffs and Class Members as a result of a breach.

62. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's server(s), amounting to potentially over two million individuals' detailed, Private Information, and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

63. The injuries to Plaintiffs and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the Private Information of Plaintiffs and Class Members.

64. The ramifications of Defendant's failure to keep secure the Private Information of Plaintiffs and Class Members are long lasting and severe. Once Private Information is stolen—particularly Social Security numbers and protected healthcare information (“PHI”)—fraudulent use of that information and damage to victims may continue for years.

65. As a largescale newspaper and journalism company in possession of its swaths of employee and subscriber Private Information, Defendant knew, or should have known, the importance of safeguarding the Private Information entrusted to them by Plaintiffs and Class Members and of the foreseeable consequences if its data security systems were breached. This includes the significant costs imposed on Plaintiffs and Class Members as a result of a breach.

Nevertheless, Defendant failed to take adequate cybersecurity measures to prevent the Data Breach.

Value of Private Information

66. The Federal Trade Commission (“FTC”) defines identity theft as “a fraud committed or attempted using the identifying information of another person without authority.”¹⁶ The FTC describes “identifying information” as “any name or number that may be used, alone or in conjunction with any other information, to identify a specific person,” including, among other things, “[n]ame, Social Security number, date of birth, official State or government issued driver’s license or identification number, alien registration number, government passport number, employer or taxpayer identification number.”¹⁷

67. The personal identifying information (“PII”) of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials.¹⁸

68. For example, Personal Information can be sold at a price ranging from \$40 to \$200.¹⁹ Criminals can also purchase access to entire company data breaches from \$900 to \$4,500.²⁰

69. Social Security numbers, which were compromised for some of the Class Members, for example, are among the worst kind of PII to have stolen because they may be put to a variety

¹⁶ 17 C.F.R. § 248.201 (2013).

¹⁷ *Id.*

¹⁸ *Your personal data is for sale on the dark web. Here's how much it costs*, Digital Trends, Oct. 16, 2019, available at: <https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/>

¹⁹ *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, available at: <https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/>

²⁰ *In the Dark*, VPNOversight, 2019, available at: <https://vpnoversight.com/privacy/anonymous-browsing/in-the-dark/>

of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.

70. What's more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

71. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, “[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number.”

72. Theft of PHI, which also occurred in this Data Breach, is also gravely serious: “[a] thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected.”²¹

²¹ *Medical I.D. Theft,* EFraudPrevention
<https://efraudprevention.net/home/education/?a=187#:~:text=A%20thief%20may%20use%20your,credit%20report%20may%20be%20affected.>

73. According to account monitoring company LogDog, medical data sells for \$50 and up on the Dark Web.²²

74. “Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery,” reported Pam Dixon, executive director of World Privacy Forum. “Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief’s activities.”²³

75. A study by Experian found that the average cost of medical identity theft is “about \$20,000” per incident and that most victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive to restore coverage.²⁴ Almost half of medical identity theft victims lose their healthcare coverage as a result of the incident, while nearly one-third of medical identity theft victims saw their insurance premiums rise, and 40 percent were never able to resolve their identity theft at all.²⁵

76. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to “close” and difficult, if not impossible, to change—names, Social Security numbers, and PHI.

²² Lisa Vaas, *Ransomware Attacks Paralyze, and Sometimes Crush, Hospitals*, Naked Security (Oct. 3, 2019), <https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals/#content>

²³ Michael Ollove, “The Rise of Medical Identity Theft in Healthcare,” Kaiser Health News, Feb. 7, 2014, <https://khn.org/news/rise-of-identity-theft/>

²⁴ See Elinor Mills, “Study: Medical Identity Theft is Costly for Victims,” CNET (Mar. 3, 2010), <https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/>

²⁵ *Id.*; see also *Healthcare Data Breach: What to Know About them and What to Do After One*, EXPERIAN, <https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-one/>

77. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, “Compared to credit card information, personally identifiable information . . . [is] worth more than 10x on the black market.”²⁶

78. Among other forms of fraud, identity thieves may obtain driver’s licenses, government benefits, medical services, and housing or even give false information to police.

79. The fraudulent activity resulting from the Data Breach may not come to light for years. There may be a time lag between when harm occurs versus when it is discovered, and also between when Private Information is stolen and when it is used. According to the U.S. Government Accountability Office (“GAO”), which conducted a study regarding data breaches:

[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.²⁷

80. Plaintiffs and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their Private Information.

Defendant Fails To Comply With FTC Guidelines

81. The Federal Trade Commission (“FTC”) has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices.

²⁶ Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), available at: <https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html>

²⁷ Report to Congressional Requesters, GAO, at 29 (June 2007), available at: <https://www.gao.gov/assets/gao-07-737.pdf>

According to the FTC, the need for data security should be factored into all business decision-making.

82. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. These guidelines note that businesses should protect the personal information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.²⁸

83. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.²⁹

84. The FTC further recommends that companies not maintain Private Information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

85. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect consumer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential Private Information as

²⁸ *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016). Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf

²⁹ *Id.*

an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act (“FTCA”), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

86. These FTC enforcement actions include actions against software companies, like Defendant.

87. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits “unfair . . . practices in or affecting commerce,” including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect Private Information. The FTC publications and orders described above also form part of the basis of Defendant’s duty in this regard.

88. Defendant failed to properly implement basic data security practices.

89. Defendant’s failure to employ reasonable and appropriate measures to protect against unauthorized access to its employees’ and subscribers’ Private Information or to comply with applicable industry standards constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

90. Upon information and belief, Defendant was at all times fully aware of its obligation to protect the Private Information of its employees and subscribers, Defendant was also aware of the significant repercussions that would result from its failure to do so. Accordingly, Defendant’s conduct was particularly unreasonable given the nature and amount of Private Information it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiffs and the Class.

Defendant Fails To Comply With HIPAA Guidelines

91. Defendant is a covered business associate under HIPAA (45 C.F.R. § 160.102) and is required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E (“Standards for Privacy of Individually Identifiable Health Information”), and Security Rule (“Security Standards for the Protection of Electronic Protected Health Information”), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

92. Defendant is subject to the rules and regulations for safeguarding electronic forms of medical information pursuant to the Health Information Technology Act (“HITECH”).³⁰ See 42 U.S.C. §17921, 45 C.F.R. § 160.103.

93. HIPAA’s Privacy Rule or *Standards for Privacy of Individually Identifiable Health Information* establishes national standards for the protection of health information.

94. HIPAA’s Privacy Rule or *Security Standards for the Protection of Electronic Protected Health Information* establishes a national set of security standards for protecting health information that is kept or transferred in electronic form.

95. HIPAA requires “compl[iance] with the applicable standards, implementation specifications, and requirements” of HIPAA “with respect to electronic protected health information.” 45 C.F.R. § 164.302.

96. “Electronic protected health information” is “individually identifiable health information ... that is (i) transmitted by electronic media; maintained in electronic media.” 45 C.F.R. § 160.103.

97. HIPAA’s Security Rule requires Defendant to do the following:

³⁰ HIPAA and HITECH work in tandem to provide guidelines and rules for maintaining protected health information. HITECH references and incorporates HIPAA.

- a. Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits;
- b. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;
- c. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted; and
- d. Ensure compliance by its workforce.

98. HIPAA also requires Defendant to “review and modify the security measures implemented ... as needed to continue provision of reasonable and appropriate protection of electronic protected health information.” 45 C.F.R. § 164.306(e). Additionally, Defendant is required under HIPAA to “[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights.” 45 C.F.R. § 164.312(a)(1).

99. HIPAA and HITECH also obligated Defendant to implement policies and procedures to prevent, detect, contain, and correct security violations, and to protect against uses or disclosures of electronic protected health information that are reasonably anticipated but not permitted by the privacy rules. *See* 45 C.F.R. § 164.306(a)(1) and § 164.306(a)(3); *see also* 42 U.S.C. §17902.

100. The HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, also requires Defendant to provide notice of the Data Breach to each affected individual “without unreasonable delay and *in no case later than 60 days following discovery of the breach.*”³¹

101. HIPAA requires a business associate to have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the business associate or the requirements of 45 C.F.R. Part 164, Subparts D or E. *See* 45 C.F.R. § 164.530(e).

102. HIPAA requires a business associate to mitigate, to the extent practicable, any harmful effect that is known to the business associate of a use or disclosure of protected health information in violation of its policies and procedures or the requirements of 45 C.F.R. Part 164, Subpart E by the covered entity or its business associate. *See* 45 C.F.R. § 164.530(f).

103. HIPAA also requires the Office of Civil Rights (“OCR”), within the Department of Health and Human Services (“HHS”), to issue annual guidance documents on the provisions in the HIPAA Security Rule. *See* 45 C.F.R. §§ 164.302-164.318. For example, “HHS has developed guidance and tools to assist HIPAA covered entities in identifying and implementing the most cost effective and appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of e-PHI and comply with the risk analysis requirements of the Security Rule.” US Department of Health & Human Services, Security Rule Guidance Material.³² The list of resources includes a link to guidelines set by the National Institute of Standards and Technology (NIST), which OCR says “represent the industry standard for good

³¹ Breach Notification Rule, U.S. Dep’t of Health & Human Services, <https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html> (emphasis added).

³² <http://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html>.

business practices with respect to standards for securing e-PHI.” US Department of Health & Human Services, Guidance on Risk Analysis.³³

Defendant Fails To Comply With Industry Standards

104. As noted above, experts studying cyber security routinely identify software companies in possession of Private Information as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

105. Several best practices have been identified that, at a minimum, should be implemented by software companies in possession of Private Information, like Defendant, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data and limiting which employees can access sensitive data. Defendant failed to follow these industry best practices, including a failure to implement multi-factor authentication.

106. Other best cybersecurity practices that are standard in the software industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points. Defendant failed to follow these cybersecurity best practices, including failure to train staff.

107. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation

³³

<https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html>

PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

108. These foregoing frameworks are existing and applicable industry standards in the software industry, and upon information and belief, Defendant failed to comply with at least one—or all—of these accepted standards, thereby opening the door to the threat actor and causing the Data Breach.

CLASS ALLEGATIONS

109. As a result of Defendant's ineffective and inadequate data security practices, the Data Breach, and the foreseeable consequences of Private Information ending up in the possession of criminals, the risk of identity theft to the Plaintiffs and Class Members has materialized and is imminent, and Plaintiffs and Class Members have all sustained actual injuries and damages, including: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

The Data Breach Increases Plaintiffs' & Class Members' Risk Of Identity Theft

110. The unencrypted Private Information of Plaintiffs and Class Members will end up for sale on the dark web as that is the *modus operandi* of hackers.

111. Unencrypted Private Information may also fall into the hands of companies that will use the detailed Private Information for targeted marketing without the approval of Plaintiffs and Class Members. Simply, unauthorized individuals can easily access the Private Information of Plaintiffs and Class Members.

112. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal Private Information to monetize the information. Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

113. Plaintiffs' and Class Members' Private Information is of great value to hackers and cyber criminals, and the data stolen in the Data Breach has been used and will continue to be used in a variety of sordid ways for criminals to exploit Plaintiffs and Class Members and to profit off their misfortune.

114. One such example of criminals piecing together bits and pieces of compromised PII for profit is the development of “Fullz” packages.³⁴

³⁴ “Fullz” is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off of those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to \$100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even “dead Fullz,” which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a “mule account” (an account that will accept a fraudulent money transfer from a compromised account) without the victim’s knowledge. See, e.g., Brian Krebs, *Medical Records for Sale in Underground*

115. With “Fullz” packages, cyber-criminals can cross-reference two sources of Private Information to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals.

116. The development of “Fullz” packages means here that the stolen Private Information from the Data Breach can easily be used to link and identify it to Plaintiffs’ and Class Members’ phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the Private Information that was exfiltrated in the Data Breach, criminals may still easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

117. The existence and prevalence of “Fullz” packages means that the Private Information stolen from the data breach can easily be linked to the unregulated data (like phone numbers and emails) of Plaintiffs and the other Class Members.

118. Thus, even if certain information (such as driver’s license numbers numbers) was not stolen in the data breach, criminals can still easily create a comprehensive “Fullz” package.

119. Then, this comprehensive dossier can be sold—and then resold in perpetuity—to crooked operators and other criminals (like illegal and scam telemarketers).

Loss Of Time To Mitigate The Risk Of Identity Theft And Fraud

Stolen From Texas Life Insurance Firm, Krebs on Security (Sep. 18, 2014), [https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-\]\(https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-finn/](https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-)

120. As a result of the recognized risk of identity theft, when a Data Breach occurs, and an individual is notified by a company that their Private Information was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft or fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm – yet, the resource and asset of time has been lost.

121. Thus, due to the actual and imminent risk of identity theft, Defendant instructs, in its Notice Letter, Plaintiffs and Class Members to take simply take precautions.³⁵

122. Plaintiffs and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions, such as researching and verifying the legitimacy of the Data Breach, contacting Philadelphia Inquirer to obtain more information about the Data Breach's occurrence, contacting financial institutions to sort out fraudulent charges on their accounts, and replacing impacted credit cards.

123. Plaintiffs' mitigation efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."³⁶

124. Plaintiffs' mitigation efforts are also consistent with the steps that FTC recommends that data breach victims take several steps to protect their personal and financial

³⁵ Notice Letter.

³⁶ See United States Government Accountability Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (June 2007), <https://www.gao.gov/new.items/d07737.pdf>.

information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.³⁷

125. And for those Class Members who experience actual identity theft and fraud, the United States Government Accountability Office released a report in 2007 regarding data breaches (“GAO Report”) in which it noted that victims of identity theft will face “substantial costs and time to repair the damage to their good name and credit record.”^[4]

Diminution Of Value Of PII and PHI

126. PII and PHI are valuable property rights.³⁸ Their value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

127. Sensitive PII can sell for as much as \$363 per record according to the Infosec Institute.³⁹

128. An active and robust legitimate marketplace for PII also exists. In 2019, the data brokering industry was worth roughly \$200 billion.⁴⁰

³⁷ See Federal Trade Commission, *Identity Theft.gov*, <https://www.identitytheft.gov/Steps>

³⁸ See “Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown,” p. 2, U.S. Government Accountability Office, June 2007, <https://www.gao.gov/new.items/d07737.pdf> (“GAO Report”).

³⁹ See, e.g., John T. Soma, et al, Corporate Privacy Trend: The “Value” of Personally Identifiable Information (“PII”) Equals the “Value” of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) (“Private Information, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.”) (citations omitted).

⁴⁰ See Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), <https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/>

129. In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.^{41,42}

130. Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to \$50.00 a year.⁴³

131. According to account monitoring company LogDog, medical data sells for \$50 and up on the Dark Web.⁴⁴

132. As a result of the Data Breach, Plaintiffs' and Class Members' Private Information, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its compromise and unauthorized release. However, this transfer of value occurred without any consideration paid to Plaintiffs or Class Members for their property, resulting in an economic loss. Moreover, the Private Information is now readily available, and the rarity of the Data has been lost, thereby causing additional loss of value.

133. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the Private Information of Plaintiffs and Class Members, and of the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiffs and Class Members as a result of a breach.

⁴¹ <https://www.latimes.com/business/story/2019-11-05/column-data-brokers>

⁴² <https://datacoup.com/>

⁴³ <https://digi.me/what-is-digime/>

⁴⁴ Lisa Vaas, *Ransomware Attacks Paralyze, and Sometimes Crush, Hospitals*, Naked Security (Oct. 3, 2019), <https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals/#content>

134. The fraudulent activity resulting from the Data Breach may not come to light for years.

135. Plaintiffs and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their Private Information .

136. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendants network, amounting to potentially over two million individuals' detailed personal information and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

137. The injuries to Plaintiffs and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the Private Information of Plaintiffs and Class Members.

Future Cost Of Credit And Identity Theft Monitoring Is Reasonable And Necessary

138. Given the type of targeted attack in this case, sophisticated criminal activity, and the type of Private Information involved, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/dark web for sale and purchase by criminals intending to utilize the Private Information for identity theft crimes –e.g., opening bank accounts in the victims' names to make purchases or to launder money; file false tax returns; take out loans or lines of credit; or file false unemployment claims.

139. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that his or her Private Information was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected

fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

140. Consequently, Plaintiffs and Class Members are at an increased risk of fraud and identity theft for many years into the future.

141. The retail cost of credit monitoring and identity theft monitoring can cost around \$200 a year per Class Member. This is a reasonable and necessary cost to monitor to protect Class Members from the risk of identity theft that arose from Defendant's Data Breach.

Loss of Benefit of the Bargain

142. Furthermore, Defendant's poor data security deprived Plaintiffs and Class Members of the benefit of their bargain. When agreeing to subscribe to Defendant's newspaper, reasonable consumers understood and expected that Defendant would properly safeguard and protect their Private Information, when in fact, Defendant did not provide the expected data security. Similarly, when applying for employment and agreeing to work on Defendant's behalf, reasonable applicants understood and expected that Defendant would properly safeguard and protect their Private Information. Accordingly, Plaintiffs and Class Members received services of a lesser value than what they reasonably expected to receive under the bargains they struck with Defendant.

Plaintiff Christopher Devine's Experience

143. Upon Information and belief, Defendant obtained Plaintiff Devine's private information through his previous employment with The Philadelphia Inquirer.

144. As a condition of his employment with Defendant, Plaintiff was required to provide Defendant, directly or indirectly, with his Private Information, including his name, address, phone number, email address, Social Security number, healthcare information, and payment information.

145. Upon information and belief, at the time of the Data Breach, Defendant retained Plaintiff's Private Information in its system.

146. Plaintiff is very careful about sharing his sensitive Private Information. Plaintiff stores any documents containing his Private Information in a safe and secure location. He has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

147. Plaintiff received the Notice Letter, by U.S. mail, directly from Defendant, dated April 29, 2024, informing him that his Private Information was improperly accessed and obtained by unauthorized third parties during the Data Breach.

148. As a result of the Data Breach and at the direction of the Notice Letter, Plaintiffs made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to: researching and verifying the legitimacy of the Data Breach, communicating with his financial and insurance services providers to alert them of the breach and learn more about precautions he can take, and changing account passwords for all of his accounts tied to sensitive personal information. Plaintiff has spent significant time on activities in response to the Data Breach—valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

149. Plaintiff suffered actual injury from having his Private Information compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of his Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal

damages; and (ix) the continued and certainly increased risk to his Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

150. Plaintiff also suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails, which, upon information and belief, was caused by the Data Breach.

151. The Data Breach has caused Plaintiff to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully informed him of key details about the Data Breach's occurrence.

152. As a result of the Data Breach, Plaintiff anticipates spending considerable time on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

153. As a result of the Data Breach, Plaintiff is at a present risk and will continue to be at a substantially increased risk of identity theft and fraud for years to come.

154. Plaintiff has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Steven Hassell's Experience

155. Plaintiff Steven Hassell is an adult individual who at all relevant times has been a citizen and resident of Philadelphia, Pennsylvania.

156. At all times material hereto, Plaintiff was Defendants' employee at The Philadelphia Inquirer.

157. As a condition of his employment at The Philadelphia Inquirer, Plaintiff was required to supply Defendants with his PII—including, but not limited to his full name, date of birth, Social Security number, and other sensitive information.

158. Plaintiff greatly values his privacy and is very careful about sharing his sensitive PII. Plaintiff diligently protects his PII and stores any documents containing PII in a safe and secure location. He has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

159. Plaintiff would not have entrusted his PII to Defendants had he known of Defendants' lax data security policies or that his PII would be maintained using inadequate data security systems.

160. At the time of the Data Breach—in or around May 2023—Defendants retained Plaintiff's PII in their computer networks.

161. Plaintiff received a written notification sent on Defendants' behalf ("Notice Letter") dated April 29, 2024 informing that his PII was accessed or exposed to unknown, unauthorized third parties through the Data Breach. According to the Notice Letter, unauthorized, unknown actors gained access to Defendants' computer network systems on or about May 11–May 13, 2023, and accessed and acquired files containing Plaintiff's sensitive PII, including his full name and Social Security number.

162. In response to the Data Breach and the Notice Letter, Plaintiff has made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach and reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud. Plaintiff monitors his financial

and credit statements multiple times a week and has already spent many hours dealing with the Data Breach, valuable time he otherwise would have spent on other activities.

163. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. Due to the Data Breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

164. Plaintiff further believes his PII, and that of Class Members, was subsequently sold on the dark web following the Data Breach, as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type. Moreover, following the Data Breach, Plaintiff has experienced suspicious spam and believes this be an attempt to secure additional PII from him.

165. In addition, Plaintiff has been informed that at least one of his private accounts has been compromised by hackers, which Plaintiff believes was hacked as a result of the Data Breach.

166. The risk of identity theft is not speculative or hypothetical, but is impending and has materialized, as there is evidence that Plaintiff and Class Members' PII was targeted, accessed, misused, and disseminated on the Dark Web.

167. Other than the Data Breach, Plaintiff is not aware of ever being part of a data breach or similar cybersecurity incident involving his PII and is concerned that it has now been exposed to bad actors.

168. Subsequent to the Data Breach, Plaintiff has suffered numerous, substantial injuries including, but not limited to: (a) financial costs incurred mitigating the materialized risk and imminent threat of identity theft; (b) loss of time and loss of productivity incurred

mitigating the materialized risk and imminent threat of identity theft; (c) financial costs incurred due to actual identity theft; (d) loss of time incurred due to actual identity theft; (e) deprivation of value of his PII; (f) invasion of privacy; and (g) the continued risk to his sensitive PII, which remains in the possession of Defendants, and which is subject to further breaches, so long as Defendants fail to undertake appropriate and adequate measures to protect the PII they collect and maintain.

169. The Data Breach has caused Plaintiff to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendants have still not fully informed him of key details about the Data Breach's occurrence or the information stolen.

Plaintiff Ivery Sheree Mosley's Experience

170. Plaintiff Mosley is a former employee at Inquirer.

171. As a condition of her employment at Inquirer, she was required to supply Defendant with her PII, including but not limited to her name and Social Security number.

172. Plaintiff Mosley is very careful about sharing her sensitive PII. Plaintiff stores any documents containing her PII in a safe and secure location. She has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

173. At the time of the Data Breach—May 11, 2023 through May 13, 2023—Defendant retained Plaintiff's PII in its system.

174. Plaintiff Mosley received the Notice Letter, by U.S. mail, directly from Defendant, dated April 29, 2024. According to the Notice Letter, Plaintiff's PII was improperly accessed and obtained by unauthorized third parties, including her full name, and Social Security number.

175. As a result of the Data Breach, and at the direction of Defendant's Notice Letter, which instructs Plaintiff to "remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors[.]"⁴⁵ Plaintiff made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to: researching and verifying the legitimacy of the Data Breach. Plaintiff have spent significant on mitigation activities in response to the Data Breach--valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

176. Subsequent to the Data Breach, Plaintiff Mosley has suffered numerous, substantial injuries including, but not limited to: (i) invasion of privacy; (ii) theft of her PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vi) statutory damages; (vii) nominal damages; and (vii) the continued and certainly increased risk to her PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

177. Plaintiff also suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails, which, upon information and belief, was caused by the Data Breach. This misuse of her PII was caused, upon information and belief, by the fact that cybercriminals are able to easily use the information compromised in the Data Breach to find

⁴⁵ Notice Letter.

more information about an individual, such as their phone number or email address, from publicly available sources, including websites that aggregate and associate personal information with the owner of such information. Criminals often target data breach victims with spam emails, calls, and texts to gain access to their devices with phishing attacks or elicit further personal information for use in committing identity theft or fraud.

178. The Data Breach has caused Plaintiff to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully informed her of key details about the Data Breach's occurrence.

179. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

180. As a result of the Data Breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

181. Plaintiff Mosley has a continuing interest in ensuring that her PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

182. **CLASS ACTION ALLEGATIONS**

183. Pursuant to Federal Rule of Civil Procedure 23, Plaintiffs propose the following Class definition, subject to amendment as appropriate:

Nationwide Class

All persons in the United States whose Private Information was maintained on Defendant's computer systems that were compromised in the Data Breach experienced by Defendant in May 2023 (the "Class").

184. Excluded from the Classes are Defendant's officers and directors, and any entity in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys,

successors, heirs, and assigns of Defendant. Excluded also from the Classes are members of the judiciary to whom this case is assigned, their families and members of their staff.

185. Plaintiffs hereby reserve the right to amend or modify the Class definition with greater specificity or division after having had an opportunity to conduct discovery.

186. Numerosity. The Members of the Class are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiffs at this time, according to the reports submitted to the Office of the Maine Attorney General, approximately 25,549 persons were impacted in the Data Breach.⁴⁶

187. Commonality. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

- a. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiffs' and Class Members' Private Information;
- b. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;
- c. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;
- d. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

⁴⁶

<https://apps.web.main.gov/online/aewviewer/ME/40/f07aadcl-ab81-4189-8f92-a3606d0b4a2e.shtml>

- e. Whether Defendant owed a duty to Class Members to safeguard their Private Information;
- f. Whether Defendant breached its duty to Class Members to safeguard their Private Information;
- g. Whether computer hackers obtained Class Members' Private Information in the Data Breach;
- h. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;
- i. Whether Plaintiffs and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;
- j. Whether Defendant's conduct was negligent;
- k. Whether Defendant breached implied contracts for adequate data security with Plaintiffs and Class Members;
- l. Whether Defendant was unjustly enriched by retention of the monetary benefits conferred on it by Plaintiffs and Class Members;
- m. Whether Defendant failed to provide notice of the Data Breach in a timely manner; and,
- n. Whether Plaintiffs and Class Members are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

188. Typicality. Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' Private Information, like that of every other Class Member, was compromised in the Data Breach.

189. Adequacy of Representation. Plaintiffs will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiffs' Counsel are competent and experienced in litigating class actions.

190. Predominance. Defendant has engaged in a common course of conduct toward Plaintiffs and Class Members, in that all the Plaintiffs' and Class Members' Private Information was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

191. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

192. Defendant has acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class-wide basis.

193. Likewise, particular issues under Fed.R.Civ.P 23(b) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

- a. Whether Defendant owed a legal duty to Plaintiffs and the Class to exercise due care in collecting, storing, and safeguarding their Private Information;
- b. Whether Defendant's security measures to protect its data systems were reasonable in light of best practices recommended by data security experts;
- c. Whether Defendant's failure to institute adequate protective security measures amounted to negligence;
- d. Whether Defendant failed to take commercially reasonable steps to safeguard consumer Private Information; and
- e. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

194. Finally, all Members of the proposed Class are readily ascertainable. Defendant has access to Class Members' names and addresses affected by the Data Breach. Class Members have already been preliminarily identified and sent Notice of the Data Incident letters by Defendant.

COUNT I
Negligence
(On behalf of Plaintiffs and the Class)

195. Plaintiffs re-allege and incorporate by reference all preceding allegations, as if fully set forth herein.

196. Defendant gathered and stored the Private Information of Plaintiffs and Class Members as part of its business of employing individuals and providing newspapers to subscribers.

197. Plaintiffs and Class Members entrusted Defendant with their Private Information with the understanding that Defendant would safeguard their information.

198. Defendant had full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiffs and Class Members could and would suffer if the Private Information were wrongfully disclosed.

199. By assuming the responsibility to collect and store this data, and in fact doing so, and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and safeguard their computer property—and Class Members' Private Information held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which they could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

200. Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

201. Defendant's duty to use reasonable security measures under HIPAA required Defendant to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(l).

Some or all of the healthcare and/or medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

202. Defendant owed a duty of care to Plaintiffs and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the Private Information.

203. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and its current and former subscribers and employees. That special relationship arose because Plaintiffs and the Class entrusted Defendant with their confidential Private Information, a necessary part of being subscribers and employees of Defendant.

204. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential Private Information.

205. Defendant was subject to an "independent duty," untethered to any contract between Defendant and Plaintiffs or the Class.

206. Defendant also had a duty to exercise appropriate clearinghouse practices to remove former employees' and subscribers' Private Information it was no longer required to retain pursuant to regulations.

207. Moreover, Defendant had a duty to promptly and adequately notify Plaintiffs and the Class of the Data Breach.

208. Defendant had and continues to have a duty to adequately disclose that the Private Information of Plaintiffs and the Class within Defendant's possession might have been

compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiffs and the Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their Private Information by third parties.

209. Defendant breached its duties, pursuant to the FTC Act, HIPAA, and other applicable standards, and thus were negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

- a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;
- b. Failing to adequately monitor the security of their networks and systems;
- c. Failure to periodically ensure that their email system had plans in place to maintain reasonable data security safeguards;
- d. Allowing unauthorized access to Class Members' Private Information;
- e. Failing to detect in a timely manner that Class Members' Private Information had been compromised;
- f. Failing to remove former employees' and subscribers' Private Information it was no longer required to retain pursuant to regulations,
- g. Failing to timely and adequately notify Class Members about the Data Breach's occurrence and scope, so that they could take appropriate steps to mitigate the potential for identity theft and other damages; and
- h. Failing to secure its stand-alone personal computers, such as the reception desk computers, even after discovery of the data breach.

210. Defendant violated Section 5 of the FTC Act and HIPAA by failing to use reasonable measures to protect Private Information and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of Private Information it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiffs and the Class.

211. Plaintiffs and the Class are within the class of persons that the FTC Act and HIPAA were intended to protect.

212. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act and HIPAA were intended to guard against.

213. Defendant's violation of Section 5 of the FTC Act and HIPAA constitutes negligence.

214. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and the Class.

215. A breach of security, unauthorized access, and resulting injury to Plaintiffs and the Class was reasonably foreseeable, particularly in light of Defendant's inadequate security practices.

216. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' Private Information would result in injury to Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the software industry.

217. Defendant has full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiffs and the Class could and would suffer if the Private Information were wrongfully disclosed.

218. Plaintiffs and the Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the Private Information of Plaintiffs and the Class, the critical importance of providing adequate security of that Private Information, and the necessity for encrypting Private Information stored on Defendant's systems.

219. It was therefore foreseeable that the failure to adequately safeguard Class Members' Private Information would result in one or more types of injuries to Class Members.

220. Plaintiffs and the Class had no ability to protect their Private Information that was in, and possibly remains in, Defendant's possession.

221. Defendant was in a position to protect against the harm suffered by Plaintiffs and the Class as a result of the Data Breach.

222. Defendant's duty extended to protecting Plaintiffs and the Class from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. See Restatement (Second) of Torts § 302B. Numerous courts and legislatures have also recognized the existence of a specific duty to reasonably safeguard personal information.

223. Defendant has admitted that the Private Information of Plaintiffs and the Class was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

224. But for Defendant's wrongful and negligent breach of duties owed to Plaintiffs and the Class, the Private Information of Plaintiffs and the Class would not have been compromised.

225. There is a close causal connection between Defendant's failure to implement security measures to protect the Private Information of Plaintiffs and the Class and the harm, or risk of imminent harm, suffered by Plaintiffs and the Class. The Private Information of Plaintiffs and the Class was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such Private Information by adopting, implementing, and maintaining appropriate security measures.

226. As a direct and proximate result of Defendant's negligence, Plaintiffs and the Class have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) experiencing an increase in spam calls, texts, and/or emails; (viii) statutory damages; (ix) nominal damages; and (x) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

227. As a direct and proximate result of Defendant's negligence, Plaintiffs and the Class have suffered and will continue to suffer other forms of injury and/or harm, including,

but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

228. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiffs and the Class have suffered and will suffer the continued risks of exposure of their Private Information, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in its continued possession.

229. Plaintiffs and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

230. Defendant's negligent conduct is ongoing, in that it still holds the Private Information of Plaintiffs and Class Members in an unsafe and insecure manner.

231. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

COUNT II
Negligence *Per Se*
(On behalf of Plaintiffs and the Class)

232. Plaintiffs re-allege and incorporate by reference all preceding allegations, as if fully set forth herein.

233. Pursuant to the Federal Trade Commission Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Private Information

234. Defendant's duty to use reasonable security measures under HIPAA required Defendant to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(l). Some or all of the healthcare and/or medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

235. Defendant breached its duties to Plaintiffs and Class Members under the Federal Trade Commission Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Private Information.

236. Defendant's failure to comply with applicable laws and regulations constitutes negligence *per se*.

237. But for Defendant's wrongful and negligent breach of their duties owed to Plaintiffs and Class Members, Plaintiffs and Class Members would not have been injured.

238. The harm resulting from the Data Breach was the harm the FTC Act and HIPAA were intended to guard against, and Plaintiffs and Class Members are within the class of persons the statute was intended to protect.

239. The injury and harm suffered by Plaintiffs and Class Members was the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that it was failing to meet its duties, and that Defendant's breach would cause Plaintiffs and Class Members to experience the foreseeable harms associated with the exposure of their Private Information.

240. As a direct and proximate result of Defendant's negligent conduct, Plaintiffs and Class Members have suffered injury and are entitled to compensatory, consequential, and punitive damages in an amount to be proven at trial.

COUNT III
Invasion of Privacy (Public Disclosure of Private Facts)
(On behalf of Plaintiffs and the Class)

241. Plaintiffs re-allege and incorporate by reference all preceding allegations, as if fully set forth herein.

242. Plaintiffs and Class Members had a reasonable expectation of privacy in the Private Information Defendant mishandled.

243. As a result of Defendant's conduct, publicity was given to Plaintiffs' and Class Members' Private Information, which necessarily includes matters concerning their private life such as PII and PHI.

244. A reasonable person of ordinary sensibilities would consider the publication of Plaintiffs' and Class Members' Private Information to be highly offensive.

245. Plaintiffs' and Class Members' Private Information is not of legitimate public concern and should remain private.

246. As such, Defendants' conduct, as alleged above, resulted in a public disclosure of private facts, for which it is liable.

247. As a direct and proximate result of Defendant's publication of their private facts, Plaintiffs and Class Members have suffered injury and are entitled to compensatory, consequential, and punitive damages in an amount to be proven at trial and any other relief allowed by law.

COUNT IV
Unjust Enrichment
(On behalf of Plaintiffs and the Class)

248. Plaintiffs re-allege and incorporate by reference all preceding allegations, as if fully set forth herein.

249. Plaintiffs and Class Members conferred a monetary benefit on Defendant. Specifically, they provided Defendant with their Private Information. In exchange, Defendant should have provided adequate data security for Plaintiffs' and Class Members'.

250. Defendant knew that Plaintiffs and Class Members conferred a benefit on it in the form their Private Information as a necessary part of their receiving services from Defendant. Defendant appreciated and accepted that benefit. Defendant profited from these transactions and used the Private Information of Plaintiffs and Class Members for business purposes.

251. Upon information and belief, Defendant funds its data security measures entirely from its general revenue, including payments on behalf of or for the benefit of Plaintiffs and Class Members.

252. As such, a portion of the payments made for the benefit of or on behalf of Plaintiffs and Class Members is to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Defendant.

253. Defendant, however, failed to secure Plaintiffs' and Class Members' Private Information and, therefore, did not provide adequate data security in return for the benefit Plaintiffs and Class Members provided.

254. Defendant would not be able to carry out an essential function of its regular business without the Private Information of Plaintiffs and Class Members and derived revenue by using it for business purposes. Plaintiffs and Class Members expected that Defendant or anyone in Defendant's position would use a portion of that revenue to fund adequate data security practices.

255. Defendant acquired the Private Information through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

256. If Plaintiffs and Class Members knew that Defendant had not reasonably secured their Private Information, they would not have allowed their Private Information to be provided to Defendant.

257. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' Personal Information. Instead of providing a reasonable level of security that would have prevented the hacking incident, Defendant instead calculated to increase its own profit at the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective security measures and diverting those funds to its own profit. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite security and the safety of their Private Information.

258. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money wrongfully obtained Plaintiffs and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

259. Plaintiffs and Class Members have no adequate remedy at law.

260. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) experiencing an increase in spam calls, texts, and/or emails; (viii) statutory damages; (ix) nominal damages; and (x) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

261. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

262. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class Members, proceeds that they unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiffs and Class Members overpaid for Defendant's services.

COUNT V
Violation of the Breach of Personal Information Notification Act (“BPINA”)
73 Pa. Stat. Ann. § 2301, *et seq.*, (West)
(On behalf of Plaintiffs and the Class)

263. Plaintiffs re-allege and incorporate by reference all preceding allegations, as if fully set forth herein.

264. Plaintiffs are “individuals” as defined by Section 2302 of the BPINA because Plaintiffs are natural persons.

265. Defendant is an “entity” as defined by Section 2302 of the BPINA because Defendant is a business doing business within the Commonwealth.

266. The Data Breach involved “Personal Information” because by Defendant’s own admission it involved: Social Security numbers, Drivers’ License numbers, State ID numbers, Financial account information, account passwords and access codes (such as PINs) and protected medical information.

267. Defendant was required under Section 2303 of the BPINA to, within a reasonable time, provide notice to any resident in the Commonwealth of Pennsylvania of an incident in which an entity reasonably believes that such resident’s personal information has been accessed and acquired by an unauthorized person.

268. Defendant became aware of the Data Breach in May 2023 when it experienced significant disruption of its network and computer systems. Shortly thereafter, Defendant received notice from the ransomware group, Cuba, that personal information belonging to Defendant’s employees and subscribers had been acquired and posted to the Dark Web.

269. Defendant failed to provide notice to its employees and subscribers that their personal information had been acquired and posted until roughly one year after Defendant initially became aware of the Data Breach.

270. Accordingly, Defendant failed to provide reasonable notice to Plaintiffs and Class Members.

271. Pursuant to Section 2308 of the BPINA, failure to comply with this statute is deemed a clear violation of the UTPCPL for which Plaintiffs and Class Members are entitled to relief under Section 201-9.2 of that statute.

COUNT VI

Violations of the Unfair Trade Practices and Consumer Protection Law (“UTPCPL”)
73 Pa. Stat. Ann. § 201-1, *et seq.*, (West)
(On behalf of Plaintiffs and the Class)

272. Plaintiffs re-allege and incorporate by reference all preceding allegations, as if fully set forth herein.

273. Plaintiffs and Defendant are “persons” as defined by Sections 201-2(2) and (11) of the UTPCPL because Plaintiffs are natural persons and Defendant is a limited liability company.

274. Defendant is involved in “trade” or “commerce” as defined by Section 201-2(3) of the UTPCPL because Defendant offers for sale or distribution news and entertainment services and newspapers throughout the Commonwealth of Pennsylvania.

275. The UTPCPL prohibits individuals or entities from engaging in “unfair methods of competitions” and “unfair or deceptive acts or practices” such as:

- a. Representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits or quantities that they do not have or that a person has a sponsorship, approval, status, affiliation or connection that he does not have;
- b. Representing that goods or services are of a particular standard, quality or grade, or that goods are of a particular style or model, if they are of another;
- c. Failing to comply with the terms of any written guarantee or warranty given to the buyer at, prior to or after a contract for the purchase of goods or services is made; and
- d. Engaging in any other fraudulent or deceptive conduct which creates a likelihood of confusion or of misunderstanding.

276. By failing to take necessary and reasonable precautions to safeguard the Private Information of Plaintiffs and Class Members, and by leading Plaintiffs and Class Members to believe that Defendant would provide adequate protection for the Private Information entrusted to it, Defendant engaged in unfair or deceptive trade practices.

277. Defendant made specific assurances to Plaintiffs and Class Members regarding its data security and disclosure practices contained within its Privacy Policy.

278. Defendant had notice of its position as a prominent news and entertainment company, the likes of which have been targeted by ransomware attacks for several years and across the globe.

279. Defendant owed common law and statutory duties to Plaintiffs and Class Members to take reasonable and adequate steps to safeguard the information it harvested from its subscribers and employees.

280. Further, Defendant owed a duty under Pennsylvania's Breach of Personal Information Notification Act to provide timely notice to Plaintiffs and Class Members that their personal information had been compromised in the Data Breach. Defendant waited nearly a full calendar year to provide this notice, however.

281. Pursuant to Section 201-9.2, Plaintiffs are entitled to the greater of actual monetary damages or \$100, treble damages under the Court's discretion, and reasonable costs and attorneys' fees.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of putative Class Members as defined above, respectfully request that this Court:

- A. Certify this case as a class action under Federal Rule of Civil Procedure 23, appoint Plaintiffs as the Class Representatives, and appoint the undersigned as Class Counsel;
- B. Order appropriate relief to Plaintiffs and the Class;
- C. Enter injunctive and declaratory relief as appropriate under the applicable law;
- D. Award Plaintiffs and the Class pre-judgment and/or post-judgment interest as prescribed by law;
- E. Award reasonable attorneys' fees and costs as permitted by law; and
- F. Enter such other and further relief as may be just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand a trial by jury on all triable issues.

Dated: July 31, 2024

Respectfully submitted,



Benjamin F. Johns
SHUB & JOHNS LLC
Four Tower Bridge
200 Barr Harbor Drive, Suite 400
Conshohocken, PA 19428
T: (610) 477-8380
bjohns@shublawyers.com

Kenneth J. Grunfeld
Jeff Ostrow
**KOPELOWITZ OSTROW FERGUSON
WEISELBERG GILBERT**
65 Overhill Road
Bala Cynwyd, PA 19004
Phone: (954) 525-4100
grunfeld@kolawyers.com
ostrow@kolawyerse.com

Terence R. Coates*
**MARKOVITS, STOCK &
DEMARCO, LLC**
119 E. Court Street, Suite 530
Cincinnati, OH 45202
Phone: (513) 651-3700
Fax: (513) 665-0219
tcoates@msdlegal.com

Gary M. Klinger*
**MILBERG COLEMAN BRYSON
PHILLIPS GROSSMAN PLLC**
227 W. Monroe Street
Suite 2100
Chicago, IL 60606
866-252-0878
gklinger@milberg.com

*admitted *pro hac vice*

Counsel for Plaintiffs and the Proposed Class

CERTIFICATE OF SERVICE

I hereby certify that on this 31st day of July 2024, I served the foregoing document upon all parties of record in this proceeding via the Court's ECF system.



Benjamin F. Johns